PGP Desktop für Windows

Schnelleinstieg
Version 9.9

Was ist PGP Desktop?

PGP Desktop bietet umfassende Sicherheit für Desktops und Laptops und ermöglicht somit Unternehmen, Arbeitsgruppen und Einzelpersonen, vertrauliche Informationen zu schützen, ohne die bestehende IT-Infrastruktur zu verändern oder Arbeitsprozesse zu stören. Diese preisgekrönte, benutzerfreundliche Lösung verschlüsselt E-Mail, Dateien, virtuelle Laufwerke und komplette Laufwerke in einer einzigen Desktop-Anwendung.

Die Anwendungen der PGP Desktop-Produktfamilie wurde in mehrere Pakete zusammengefasst.

- **PGP Desktop Professional 9.9** umfasst PGP Desktop Email und PGP Whole Disk Encryption
- **PGP Desktop Storage 9.9** umfasst PGP Whole Disk Encryption und PGP NetShare.
- **PGP Desktop Enterprise 9.9** umfasst PGP Desktop Email, PGP Whole Disk Encryption und PGP NetShare.

PGP Desktop Email

PGP Desktop Email ermöglicht die automatische und transparente Verschlüsselung, Signatur, Entschlüsselung und Verifizierung von E-Mail-Nachrichten anhand von Richtlinien, die von Administratoren für Sie festgelegt wurden, oder Richtlinien, die Ihrer Kontrolle unterliegen, wenn Sie nicht im Rahmen einer mit PGP Universal Server verwalteten Umgebung arbeiten.

PGP NetShare

Sie können mit PGP NetShare autorisierten Anwendern die Freigabe geschützter Dateien in einem freigegebenen Speicherbereich ermöglichen, z. B. auf einem Dateiserver, in einem freigegebenen Ordner oder auf einem USB-Wechseldatenträger .

PGP Whole Disk Encryption

Mit PGP Whole Disk Encryption (WDE) kann der gesamte Inhalt Ihres Systems oder eines von Ihnen angegebenen externen oder USB-Flash-Laufwerks gesperrt werden.

Darüber hinaus können Sie mit PGP Desktop folgende Aufgaben ausführen:

- Einen Teil Ihres Festplattenspeichers als verschlüsseltes virtuelles Laufwerk mit eigenem Laufwerksbuchstaben verwenden.
- Geschützte Zip-Archive erstellen.
- Dateien und Ordner in einem einzelnen, verschlüsselten und komprimierten Paket ablegen, das auf Windows-Systemen geöffnet werden kann, auf denen PGP Desktop nicht installiert ist.
- Dateien und Ordner vollständig zerstören, so dass sie auf keine Weise wiederhergestellt werden können.
- Freien Speicherplatz auf Laufwerken sicher löschen, so dass die gelöschten Daten keinesfalls wiederhergestellt werden können.

Inhalt

- *Was ist PGP Desktop?* (Seite 1)
- *Neu bei PGP Desktop?* (Seite 1)
- *Die Grundlagen* (Seite 1)
- *Was wird installiert?* (Seite 2)
- *Systemvoraussetzungen* (Seite 3)
- *PGP Desktop installieren* (Seite 3)
- *PGP Desktop starten* (Seite 4)
- *Der Hauptbildschirm von PGP Desktop* (Seite 4)
- PGP Desktop Email verwenden (Seite 4)
- PGP NetShare verwenden (Seite 6)
- PGP WDE zur Verschlüsselung eines Laufwerks verwenden (Seite 7)
- PGP Virtual Disk-Laufwerke *erstellen* (Seite 10)
- *Ein PGP Zip-Archiv erstellen* (Seite 11)
- *Dateien sicher löschen* (Seite 14)
- *Freien Speicherplatz sicher löschen* (Seite 15)
- *Hilfe und Support* (Seite 15)

Neu bei PGP Desktop?

Diese schrittweise Anleitung erleichtert Ihnen den Einstieg. Sie werden feststellen, dass der Schutz Ihrer Daten mit PGP Desktop so einfach ist wie das Drehen eines Schlüssels in einem Schloss.

- Dieser *Schnelleinstieg* enthält die Installationsanleitung für PGP Desktop und erste Schritte.
- *Das PGP Desktop Anwenderhandbuch* stellt noch detailliertere Informationen zu PGP Desktop bereit. Dort erfahren Sie, was ein Schlüsselpaar ist, wann und wie Sie ein Schlüsselpaar erstellen können und wie Sie Schlüssel mit anderen Personen austauschen können, um Ihre eigenen Daten zu verschlüsseln und Daten sicher mit anderen auszutauschen.

  Hinweis: Eine PGP Desktop-Lizenz gibt Ihnen Zugang zu einem bestimmten Satz von PGP Desktop-Funktionen. Manche anderen Funktionen von PGP Desktop können eine andere Lizenz erfordern. Nähere Informationen finden Sie im Abschnitt über Lizenzen im *PGP Desktop Anwenderhandbuch*.

- Informationen zur Implementierung, Verwaltung und Richtliniendurchsetzung für PGP Desktop finden Sie im *Administrator-Handbuch für PGP Universal Server*.

Die Grundlagen

PGP Desktop verwendet Schlüssel zur Verschlüsselung, Signatur, Entschlüsselung und Verifikation von Nachrichten.

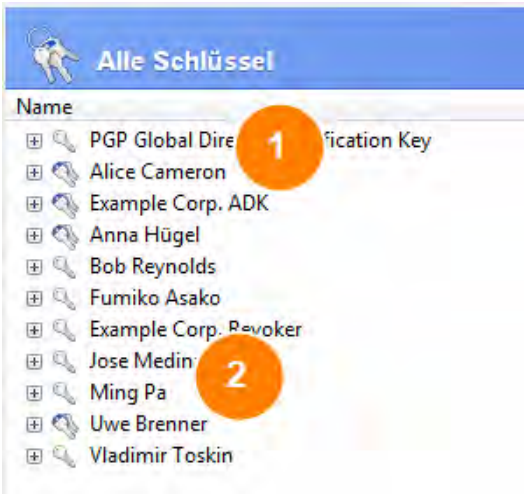
Nach der Installation werden Sie von PGP Desktop zur

Erstellung eines PGP-Schlüsselpaars aufgefordert. Ein Schlüsselpaar ist die Kombination eines privaten Schlüssels und eines öffentlichen Schlüssels.

- Wie der Name schon nahelegt, behalten Sie Ihren *privaten Schlüssel* und das zugehörige Passwort für sich. Wenn eine andere Person Ihren privaten Schlüssel und das Passwort erfährt, kann sie Ihre Nachrichten lesen und sich anderen gegenüber für Sie ausgeben. Ihr privater Schlüssel entschlüsselt eingehende verschlüsselte Nachrichten und signiert ausgehende Nachrichten.
- Ihren *öffentlichen Schlüssel* können Sie ruhig ausgeben. Er hat kein Passwort. Ihr öffentlicher Schlüssel verschlüsselt Nachrichten, die nur Ihr privater Schlüssel entschlüsseln kann und er verifiziert Ihre signierten Nachrichten.

Ihr Schlüsselbund umfasst Ihre Schlüsselpaare und die öffentlichen Schlüssel von anderen, die Sie zur Versendung von verschlüsselten Nachrichten an diese Personen verwenden. Klicken Sie auf das Bedienfeld „PGP Keys“ um die Schlüssel an Ihrem Schlüsselbund anzuzeigen:

1. Das Symbol für ein PGP-Schlüsselpaar hat zwei Schlüssel, die den privaten und den öffentlichen Schlüssel anzeigen. Alice Cameron, zum Beispiel, hat in dieser Illustration ein PGP-Schlüsselpaar.
2. Die Symbole für die öffentlichen Schlüssel von anderen haben nur einen Schlüssel. Der öffentliche Schlüssel von Ming Pa, zum Beispiel, wurde dem in dieser Illustration abgebildeten Schlüsselbund hinzugefügt.



PGP Desktop Email ist eine Anwendung der PGP Desktop-Produktfamilie. PGP Desktop Email kann auch zur automatischen und transparenten Verschlüsselung, Signatur, Entschlüsselung und Verifikation von E-Mail-Nachrichten mit Richtlinien, über die Sie Kontrolle haben, verwendet werden. PGP Desktop Email kann auch zur Verschlüsselung von IM-Sitzungen für Clients, zum Beispiel AIM und iChat, verwendet werden. Bei beiden Benutzern muss PGP Desktop Email aktiviert sein.

PGP NetShare ist eine Anwendung der PGP Desktop-Produktfamilie Mit PGP NetShare können Sie Anwendern die gemeinsame Verwendung geschützter Dateien in einem freigegebenen Speicherbereich ermöglichen, wie z. B. auf einem firmeninternen Dateiserver, in einem freigegebenen Ordner oder auf einem Wechseldatenträger (z. B. USB-Laufwerk), gemeinsam zu verwenden. Die verschlüsselten Dateien im geschützten Ordner werden den autorisierten Anwendern weiterhin als normale Anwendungsdateien präsentiert; jeder Anwender mit physischem Zugang zu den Dateien kann sie sehen, jedoch nicht benutzen.

PGP Whole Disk Encryption (WDE) ist eine Anwendungder PGP Desktop-Produktfamilie. Mit PGP Whole Disk Encryption (WDE) kann der gesamte Inhalt Ihres Systems oder eines von Ihnen angegebenen externen oder USB-Flash-Laufwerks gesperrt werden. Boot-Sektoren, Systemdateien und Auslagerungsdateien werden alle verschlüsselt. Bei kompletter Laufwerkverschlüsselung des Boot-Laufwerks brauchen Sie sich bei Verlust oder Diebstahl Ihres Computers keine Sorgen zu machen: zum Zugriff auf Ihre Daten würde ein Angreifer das entsprechende Passwort benötigen.

Was wird installiert?

PGP Desktop verwendet Lizenzen, um Zugang zu den von Ihnen erworbenen Funktionen bereitzustellen. Je nach Lizenz können einige oder alle Anwendungen der PGP Desktop-Produktfamilie genutzt werden.

Dieses Dokument enthält eine Anleitung zur Anzeige der durch Ihre Lizenz aktivierten Funktionen.

PGP Virtual Disk-Laufwerke — Verwendet einen Teil Ihres Festplattenspeichers als verschlüsseltes virtuelles Laufwerk mit seinem eigenen Laufwerksbuchstaben. Ein PGP Virtual Disk-Laufwerk ist der perfekte Speicherort für Ihre vertraulichen Dateien; sie sind dort so sicher gespeichert wie in einem Safe. Wenn die Safetür geöffnet ist (d.h. wenn das Laufwerk aktiviert ist), können Sie dort gespeicherte Dateien ändern, Dateien herausnehmen und Dateien hineinstellen. Anderenfalls (wenn das Laufwerk deaktiviert ist) sind alle Daten auf dem Laufwerk geschützt.

PGP Zip — Fügt einem verschlüsselten, komprimierten, portablen Archiv jede beliebige Kombination von Dateien und Ordnern hinzu. PGP Desktop muss auf dem System installiert sein, damit ein PGP Zip-Archiv erstellt oder geöffnet werden kann. PGP Zip ist ein Werkzeug zur sicheren Archivierung Ihrer vertraulichen Daten zum Zwecke der Verteilung an andere oder Datensicherung.

Selbstentschlüsselnde PGP-Archive (SDAs) — Platziert Dateien und Ordner in ein verschlüsseltes, komprimiertes Paket, das auf Windows-Systemen, auf denen PGP Desktop nicht installiert ist, geöffnet werden kann. SDAs sind die perfekte Lösung zum sicheren Austausch von Dateien mit einer Person, die die PGP Software nicht installiert hat.

PGP Shredder — Zur vollständigen Vernichtung von Dateien und Ordnern, so dass sie selbst mit Dateiwiederherstellungssoftware nicht wiederhergestellt werden können. Wenn eine Datei über den Windows-Papierkorb entfernt wird, wird sie nicht wirklich gelöscht; sie verbleibt auf Ihrem Laufwerk, bis sie schließlich überschrieben wird. Bis zu dem Zeitpunkt kann diese Datei leicht von einem Angreifer wiederhergestellt werden. PGP Shredder hingegen überschreibt Dateien sofort mehrfach. Das ist so effektiv, dass diese Dateien selbst mit hochentwickelter Laufwerkwiederherstellungssoftware nicht wiederhergestellt werden können. Diese Funktion löscht auch freien Speicherplatz auf Ihren Laufwerken sicher, so dass Ihre gelöschten Daten wirklich nicht wiederherstellbar sind.

Schlüsselverwaltung — PGP Desktop verwaltet auch PGP-Schlüssel, d. h. sowohl Ihre Schlüsselpaare als auch die öffentlichen Schlüssel von anderen. Sie verwenden Ihren privaten Schlüssel zur Entschlüsselung von Nachrichten, die Ihnen auf Ihren öffentlichen Schlüssel verschlüsselt zugeschickt werden, sowie zur Sicherung Ihrer PGP Virtual Disk-Laufwerke. Öffentliche Schlüssel werden zur Verschlüsselung von Nachrichten für andere Personen oder zum Hinzufügen von Anwendern zu PGP Virtual Disk-Laufwerken verwendet.

Systemvoraussetzungen

- Microsoft Windows 2000 (Servicepack 4), Windows Server 2003 (Servicepack 1), Windows XP (Servicepack 1, 2 oder 3, 32-Bit- und 64-Bit-Versionen), Windows Vista (alle 32-Bit- und 64-Bit-Versionen, einschl. Servicepack 1), Microsoft Windows XP Tablet PC Edition 2005 (angeschlossene Tastatur notwendig)

  Hinweis: Die oben aufgeführten Betriebssysteme werden nur dann unterstützt, wenn die neuesten Hotfixes und Sicherheitspatches von Microsoft installiert wurden.

  PGP Whole Disk Encryption (WDE) erfordert Windows 2000 (Servicepack 4), Windows XP (Servicepack 1 oder 2) oder Windows Vista; unter Windows 2000 Server oder 2003 Server wird es nicht unterstützt.
- 512 MB RAM
- 64 MB Festplattenspeicher

PGP Desktop installieren

PGP Corporation empfiehlt, alle geöffneten Anwendungen zu schließen, bevor die Installation gestartet wird. Der Installationsprozess erfordert einen Systemneustart.

Hinweis: Wenn Sie PGP Desktop in einer mit PGP Universal Server verwalteten Umgebung verwenden ist ist Ihre PGP Desktop-Installationssoftware möglicherweise mit spezifischen Funktionen und/oder Einstellungen konfiguriert.

➢ So installieren Sie PGP Desktop

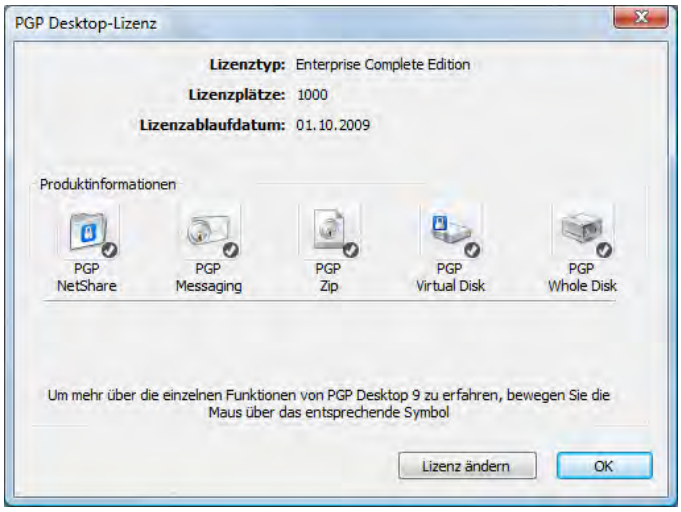
1. Suchen Sie das PGP Desktop-Installationsprogramm, das Sie heruntergeladen haben.

   Das Installationsprogramm wurde möglicherweise von Ihrem PGP-Administrator mit dem Bereitstellungstool Microsoft SMS verteilt.
2. Doppelklicken Sie auf das Installationsprogramm.
3. Folgen Sie der Anleitung auf dem Bildschirm.
4. Starten Sie das System auf die entsprechende Anweisung hin neu.
5. Befolgen Sie beim Neustart die Anweisungen auf dem

Bildschirm zur Konfiguration von PGP Desktop.

Lizenzierung

Zur Anzeige der Funktionen, die im Rahmen Ihrer Lizenz unterstützt werden, öffnen Sie PGP Desktop und wählen Sie **Hilfe > Lizenz**. Die Funktionen mit einer Kontrollmarkierung werden von der aktiven Lizenz unterstützt.



PGP Desktop starten

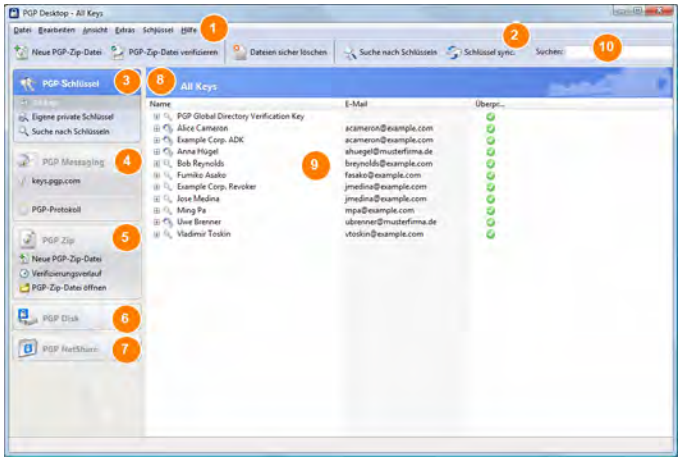
Sie können PGP Desktop auf folgende Arten starten:

- Doppelklicken Sie auf das PGP Tray-Symbol.

- Rechtsklicken Sie auf das PGP Tray-Symbol und wählen Sie dann **PGP Desktop öffnen**.
- Wählen Sie im **Start**-Menü **Programme > PGP > PGP Desktop**.

Der PGP Desktop-Hauptbildschirm

Das Anwendungsfenster von PGP Desktop ist die primäre Benutzeroberfläche für das Produkt.



Dieser Bildschirm enthält folgende Elemente:

1	**Menüleiste**. Ermöglicht den Zugriff auf PGP Desktop-Befehle. Die Zusammenstellung der Menüs auf der Menüleiste ändert sich in Abhängigkeit davon, welches Bedienfeld ausgewählt wird.
2	**Symbolleiste**. Auf diesem Steuerelement sind die am häufigsten benötigten Funktionen angeordnet. Sie können ein neues PGP Zip-Archiv erstellen, ein bestehendes PGP Zip-Archiv verifizieren, ausgewählte Dateien sicher löschen, nach einem Schlüssel suchen, Ihre Schlüssel synchronisieren und in den Anwender-IDs der Schlüssel, die gegenwärtig im Arbeitsbereich „PGP Keys“ angezeigt werden, nach Text suchen.
3	**Bedienfeld „PGP Keys“**. Mit diesem Symbol verwalten Sie die PGP-Schlüssel.
4	**Bedienfeld „PGP Messaging“**. Mit diesem Symbol steuern Sie PGP Messaging.
5	**Bedienfeld „PGP Zip“**. Mit diesem Bedienfeld steuern Sie die Funktionen von PGP Zip sowie des PGP Zip-Assistenten, der Sie bei der Erstellung neuer PGP Zip-Archive unterstützt.
6	**Bedienfeld „PGP Disk“**. Mit diesem Symbol steuern Sie PGP Disk.
7	**Bedienfeld „PGP NetShare“**. Mit diesem Symbol steuern Sie PGP NetShare.
8	**Bedienfeldsteuerung ein-/ausblenden.** Mit diesem Symbol blenden Sie die Bedienfelder ein oder aus.
9	**Arbeitsbereich von PGP Desktop**. Hier werden neben verschiedenen Informationen die Aktionen angezeigt, die Sie für das ausgewählte Bedienfeld durchführen können.

10 **Suchfeld „“PGP Keys“**. Hier können Sie nach Schlüsseln in Ihrem Schlüsselbund suchen. Wenn Sie in diesem Feld Text eingeben, zeigt PGP Desktop Suchergebnisse von Namen und E-Mail-Adressen an.

Jedes Bedienfeld kann erweitert werden, um verfügbare Optionen anzuzeigen. Standardmäßig ist es platzsparend ausgeblendet (nur das Symbol des Bedienfelds wird angezeigt). Sie können das Bedienfeld erweitern, indem Sie auf das Symbol klicken. Sie können das Bedienfeld wieder ausblenden, indem Sie auf den Pfeil „Ein-/Ausblenden“ oben rechts klicken.

PGP Desktop Email verwenden

PGP Desktop Email kann zur automatischen und transparenten Verschlüsselung und Signatur von ausgehenden Nachrichten und zur Entschlüsselung und Verifikation von eingehenden Nachrichten verwendet werden. Dazu versenden und empfangen Sie Ihre E-Mail ganz einfach wie gehabt; PGP Desktop Email übernimmt alles andere.

Verschlüsselte E-Mail-Nachrichten senden

Nach der Installation wird PGP Desktop Email zwischen Ihrem E-Mail-Client und Ihrem Mail-Server eingefügt, wo er Ihren E-Mail-Verkehr überwacht.

Beim Eingang von *eingehenden* Nachrichten werden diese von PGP Desktop Email abgefangen, bevor sie in den Posteingang gelangen, und es wird automatisch versucht, sie zu entschlüsseln und zu verifizieren; zur Entschlüsselung werden Ihre privaten Schlüssel und zur Verifikation werden Ihre öffentlichen Schlüssel verwendet. Nach Abschluss dieser Maßnahmen werden Ihre Nachrichten von PGP Desktop Email in Ihren Posteingang zugestellt.

In den meisten Fällen brauchen Sie nichts weiter zu tun; entschlüsselte eingehende Nachrichten erscheinen in Ihrem Posteingang wie alle anderen eingehenden Nachrichten.

Beim Versenden von *ausgehenden* Nachrichten werden diese auf dem Weg zu Ihrem Mail-Server von PGP Desktop Email abgefangen und es wird automatisch versucht, sie auf der Grundlage der konfigurierten Grundsätze zu verschlüsseln und zu signieren.

Auch hier brauchen Sie nichts weiter zu tun; Sie erstellen einfach Ihre Nachrichten mit Ihrem E-Mail-Client und versenden sie — PGP Desktop Email übernimmt alles weitere.

Die nachfolgenden Abschnitte enthalten detaillierte Informationen zur transparenten Handhabung Ihrer eingehenden und ausgehenden Nachrichten durch PGP Desktop Email.

Eingehende Nachrichten

PGP Desktop Email handhabt eingehende Nachrichten nach inhaltlichen Gesichtspunkten:

- **Weder verschlüsselt noch signiert**. Wenn eine Nachricht weder verschlüsselt noch signiert ist, wird sie von PGP Desktop Email einfach an Ihren E-Mail-Client weitergeleitet. Die Nachricht ist in ihrer jetzigen Form lesbar, so dass PGP Desktop Email nichts weiter tun muss.
- **Verschlüsselt, jedoch nicht signiert**. Wenn eine Nachricht verschlüsselt ist, versucht PGP Desktop Email, sie zu entschlüsseln, so dass sie gelesen werden kann. Zuerst wird Ihr Schlüsselbund nach dem privaten Schlüssel, der die Nachricht entschlüsseln kann, abgesucht. Wird der private Schlüssel gefunden, entschlüsselt PGP Desktop Email damit die Nachricht und leitet sie dann an Ihren E-Mail-Client weiter. Wenn der private Schlüssel nicht gefunden wird, leitet PGP Desktop Email die Nachricht verschlüsselt an Ihren E-Mail-Client weiter. Das sieht dann ungefähr so aus.

```
-----BEGIN PGP MESSAGE -----
Version: PGP Desktop 9.9

qANQR1DBwUwDMvpGQkaZ1HwBD/0f5F8QKtY+1NvzwQW4xQ/EPu0D0mLrMZVVNQVn
rYvHPoSAcn6C3zFpO996akjRioOBGa62hkLpkjQi3QEGpBtqMP1F64TUxqHkpLNH
ISN+7zEA7EYTtV+3ErREOH6yQgJ+sQGm6sjRjddYYvTG6hGa9f2wX+ZDLAIK65rA
f4ZNQfNvkowMmJXS78Sz7LEGE5d5WM68kKB/FflvfYz1w36OQgauIXmom9F8294p
fNaWAnhQlRif/la/MuYs0WkTLPQpdBXhgZqVKaE85gsCrWqXfMAGDEYfrsCAb1Ne
nMWJNtXsRYVpstmpNBZuVHOljKrXE4YEAPk48MOD1Yi54NJxYwvury79oDoxDljh
o9yh9v5f071orpLFcew8wmLX4qJaGds0VqdwQRRnfwbwnbgsdljD2cmijyOq+bcy
3hZknIEGbb7GTKaKo1cj+y9uSaFDh49lA9qLyHTWwLuHYV/j/wtBPfPZpjGYvACV
FqRDEO8hYzxKc/foQwlIMdo+nymZEQItTTdBCaESxm5v+jBwfn0xhUK/EVylkAHm
n27x2m9PdwzxriQjgrxI8Lda7DTJWYmA8ol2OClQZqrqvAmqIKL4CpCkyhPuRwIg
nan80KN/USfzK+Vi9juxM1lS5oGYz0DtL6KnLnGGpTlu6yLsU2SB7iIbVe330ukj
zMLXgdLAKQFSItPMVeKqJPxQrMrLlEYr6hE7fCAYmUMwXe8w60e7H2OwEIme2Y9V
eVocs5p9Iau7w987Ifbh1odEb+QEwJMaVV5jBcaE1ZhxAYLfrIdXBb1REeuQGjmj
FuCHf6BGgTp9HlNjw92iR5qSintROh2KmwTa5oGbDNnEEAAQJp8sI+6129FLpLgF
z7/wzmnKFngV4OgILxyPCRvS6Pbo30wAgJehhqDzC9kEkmXd6J7t/caDEMUsnHC1
qTBAScHRB+8eN5yrUrZ5YUqhNvpR/vVN6odPEnX4mbrMsClv4uXRYSv5ofGHJT0U
=8hvs
-----END PGP MESSAGE -----
```

- **Signiert, jedoch nicht verschlüsselt**. Wenn eine Nachricht signiert ist, versucht PGP Desktop Email, die Signatur zu überprüfen. Die folgenden Speicherorte werden in dieser Reihenfolge auf den entsprechenden öffentlichen Schlüssel hin abgesucht: Ihr Standardschlüssel, der Keyserver auf keys.domain, wobei Domain die Domain des Absenders der Nachricht ist, das PGP Global Directory (keyserver.pgp.com), alle anderen konfigurierten Keyserver. Wenn PGP Desktop Email den entsprechenden öffentlichen Schlüssel findet, versucht es, die Signatur zu überprüfen und dann die Nachricht an Ihren E-Mail-Client weiterzuleiten. Falls PGP Desktop den entsprechenden öffentlichen Schlüssel nicht findet, wird die Nachricht unverifiziert an Ihren E-Mail-Client übergeben.
- **Verschlüsselt und signiert**. Wenn eine Nachricht verschlüsselt und signiert ist, versucht PGP Desktop Email zuerst, den privaten Schlüssel zur Entschlüsselung der Nachricht und dann den öffentlichen Schlüssel zur Verifizierung der Nachricht zu finden.

Ausgehende Nachrichten

PGP Desktop Email handhabt Ihre abgehenden E-Mail-Nachrichten auf der Grundlage von Richtlinien bzw. Anleitungssätzen, die zur Handhabung jeder Situation festgelegt werden können.

Standardrichtlinien

PGP Desktop Email umfasst vier Standardrichtlinien:

- **Mailing-Listen-Administratorabfragen**. Administratorabfragen an Mailing-Listen sollen als Klartext gesendet werden; d.h. weder verschlüsselt noch signiert.

- **Mailing-Listen-Sendevorgänge**. Sendevorgänge werden an Mailing-Listen signiert (damit sie authentifiziert werden können), jedoch nicht verschlüsselt gesendet.
- **Verschlüsselung erzwingen: [PGP] Vertraulich**. Alle als vertraulich markierten Nachrichten in Ihrem E-Mail-Client, oder die den Text „[PGP]" in der Betreffzeile enthalten, müssen an einen gültigen öffentlichen Schlüssel eines Empfängers verschlüsselt werden, damit sie gesendet werden können. Diese Richtlinie gibt Ihnen ein Verfahren zur einfachen Handhabung von Nachrichten, die verschlüsselt gesendet werden *müssen*; sonst werden sie nicht gesendet.
- **Opportunistische Verschlüsselung** Legt fest, dass alle Nachrichten, für die kein Verschlüsselungsschlüssel gefunden wird, unverschlüsselt (als Klartext) gesendet werden. Wenn sich diese Richtlinie als letzte Richtlinie in der Liste befindet, wird gewährleistet, dass Ihre Nachrichten immer gesendet werden (außer wenn sie als vertraulich markiert werden) (wenn auch als Klartext), selbst wenn kein Schlüssel zur Verschlüsselung für den Empfänger gefunden wird.

Neue Richtlinien erstellen

PGP Desktop Email bietet die Möglichkeit zusätzlich zu den vier Standardrichtlinien neue Richtlinien zu erstellen und zu verwenden . Sie können Richtlinien auf der Grundlage vieler verschiedener Kriterien erstellen.

Vollständige Informationen zur Erstellung und Implementierung von Messaging-Richtlinien finden Sie im *PGP Desktop Anwenderhandbuch*.

Wurde meine Nachricht verschlüsselt?

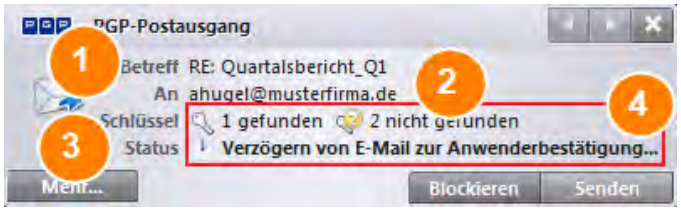
Da PGP Desktop Email seine Arbeit automatisch und transparent vollzieht, kann es vorkommen, dass Sie sich fragen, ob Ihre Nachricht wirklich verschlüsselt versendet wurde. Das ist aller Wahrscheinlichkeit nach der Fall, aber es gibt auch Möglichkeiten, das sicherzustellen.

Notifier-Warnungen

PGP Desktop Notifier-Warnungen sind eine Funktion von PGP Desktop Email, die Ihnen Einzelheiten zum Messaging mitteilt und Ihnen gleichzeitig Kontrolle darüber gibt.

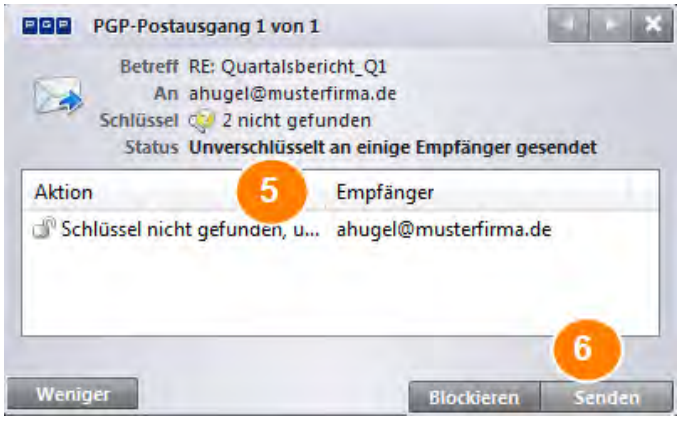
Wenn Sie zum Beispiel eine verschlüsselte Nachricht versenden, erscheint in der rechten unteren Ecke des Bildschirms die Notifier-Warnung. Sie enthält folgende Einzelheiten:

1. Betreff:
2. Empfänger der Nachricht
3. Für den Empfänger gefundene Schlüssel
4. Status der Nachricht



Wenn Sie mehr Informationen über die versandte Nachricht sehen wollen, klicken Sie auf **Mehr**. Daraufhin werden auch folgende Informationen angezeigt:

5. Was PGP Desktop Email mit der Nachricht gemacht hat
6. Wer die Nachricht signiert hat



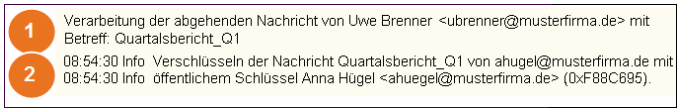
Nähere Informationen über Notifiers finden Sie im *Benutzerhandbuch für PGP Desktop*.

PGP Log-Datei

In der PGP Log-Datei sind verschiedene Maßnahmen aufgelistet, die PGP Desktop Email zum Schutz Ihres Messaging ergreift.

Zum Beispiel hat die Nachricht, deren Notifiers oben aufgezeigt sind, diesen Eintrag in der PGP Log-Datei erzeugt. Er enthält folgende Einzelheiten:

1. Dass eine abgehende Nachricht gesendet wurde, Absender und Betreff der Nachricht
2. Uhrzeit der Verschlüsselung; E-Mail-Adresse, an die die Verschlüsselung erfolgte; und die E-Mail-Adresse des Absenders

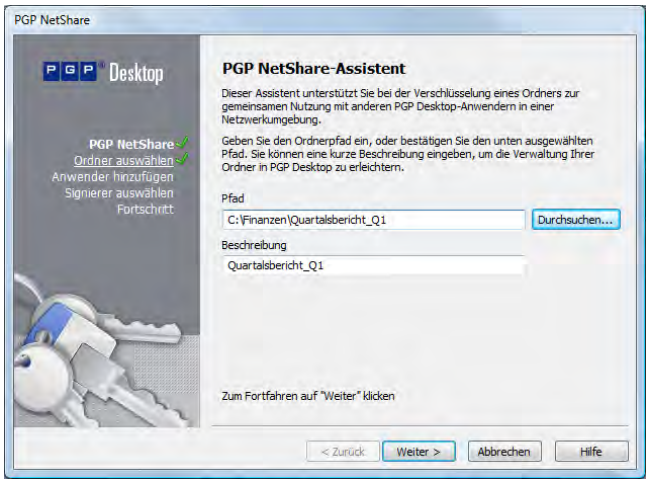


PGP NetShare verwenden

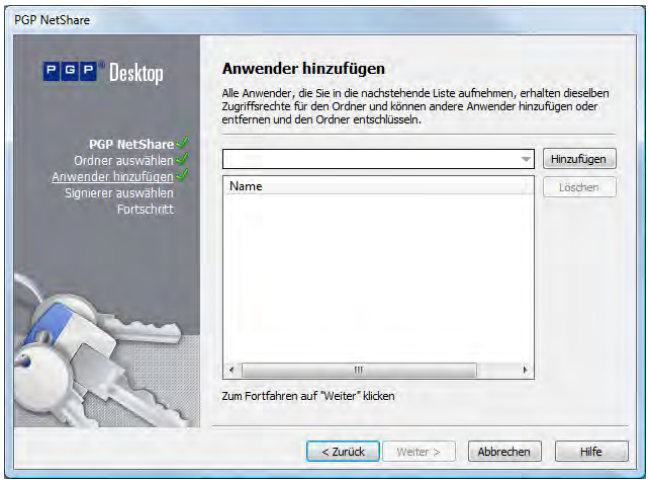
Die PGP NetShare-Funktion ermöglicht autorisierten Anwendern die gemeinsame Benutzung von geschützten Dateien. Sie müssen zuerst einen geschützten Ordner erstellen und die Anwender spezifizieren, die zur Benutzung der Dateien autorisiert sein sollen.

1. Klicken Sie im Bedienfeld „PGP NetShare“ auf **Ordner hinzufügen**.

Das Fenster „Ordner auswählen“ wird geöffnet.


PGP NetShare
PGP Desktop
PGP NetShare
Ordner auswählen
Anwender hinzufügen
Signierer auswählen
Fortschritt
PGP NetShare-Assistent
Dieser Assistent unterstützt Sie bei der Verschlüsselung eines Ordners zur gemeinsamen Nutzung mit anderen PGP Desktop-Anwendern in einer Netzwerkumgebung.
Geben Sie den Ordnerpfad ein, oder bestätigen Sie den unten ausgewählten Pfad. Sie können eine kurze Beschreibung eingeben, um die Verwaltung Ihrer Ordner in PGP Desktop zu erleichtern.
Pfad
C:\Finanzen\Quartalsbericht_Q1
Durchsuchen...
Beschreibung
Quartalsbericht_Q1
Zum Fortfahren auf "Weiter" klicken
< Zurück
Weiter >
Abbrechen
Hilfe

2. Klicken Sie auf **Durchsuchen** und wählen Sie dann den Ordner, den Sie als geschützten Ordner ausersehen haben.
3. Geben Sie im Feld **Beschreibung** eine Beschreibung für den erstellten geschützten Ordner ein oder lassen Sie es frei, um den Standardnamen zu verwenden.
4. Klicken Sie auf **Weiter**. Das Fenster „Benutzer hinzufügen“ wird angezeigt.



5. Zur Angabe von Benutzern der Dateien im geschützten Ordner klicken Sie auf den Abwärtspfeil, wählen einen Anwender aus und klicken dann auf **Hinzufügen**. Denken Sie daran, sich selbst hinzuzufügen, wenn Sie auf die Dateien im geschützten Ordner zugreifen wollen.

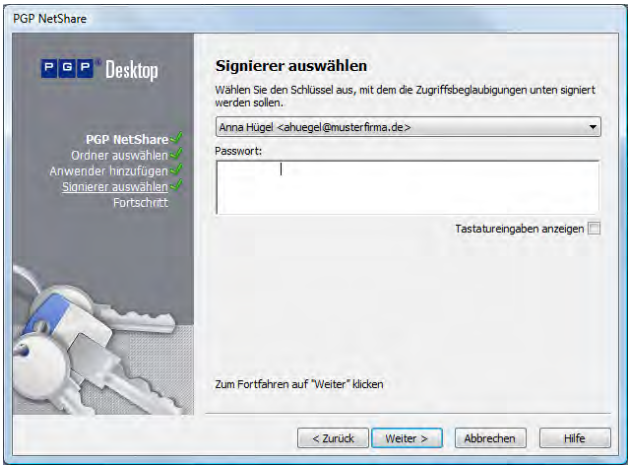
PGP NetShare teilt den Anwendern nicht mit, dass sie auf die geschützten Dateien zugreifen können; es obliegt dem Ersteller eines neuen geschützten Ordners, Benutzer zu benachrichtigen.

6. Sie können den einzelnen Anwendern Rollen zuweisen, indem Sie mit der rechten Maustaste auf den jeweiligen Anwendernamen klicken und eine Rolle auswählen:

- **Administrator**: Erstellen Sie nur eine Administrator-Rolle pro geschütztem PGP NetShare-Ordner. Diese Rolle verfügt über volle Lese-/Schreibrechte am Ordner; sie ermöglicht das Hinzufügen und Entfernen von Benutzern, die Zuweisung von Rollen sowie die Ernennung eines anderen Benutzers zum Admin.
- **Gruppen-Administrator**: Für jeden geschützten PGP NetShare-Ordner können Sie beliebig viele Gruppen-Administratoren einrichten. Diese Rolle verfügt über volle Lese-/Schreibrechte am Ordner, sie ermöglicht das Hinzufügen und Entfernen von Benutzern und die Zuweisung von Rollen.
- **Anwender**: Für jeden geschützten PGP NetShare-Ordner können Sie beliebig viele Anwender einrichten. Diese Rolle verfügt über volle Lese-/Schreibrechte am Ordner.

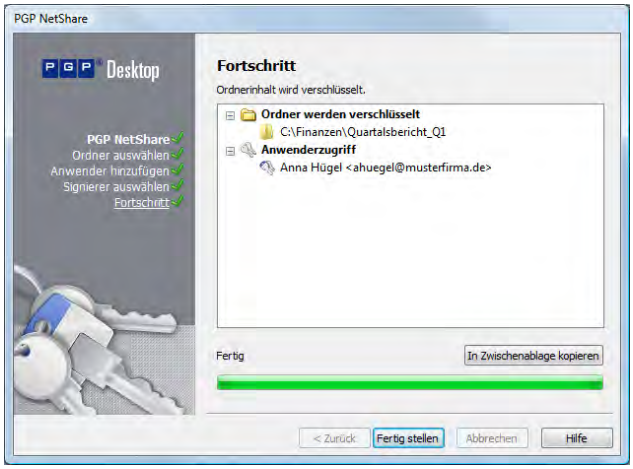
Sie können die Rolle eines Anwenders jederzeit nach Erstellung des geschützten Ordners ändern. Klicken Sie in PGP Desktop auf den geschützten Ordner und anschließend mit der rechten Maustaste auf den Anwendernamen, um die Rolle dieses Anwenders zu ändern.

7. Klicken Sie auf **Weiter**. Das Fenster „Signierer auswählen“ wird geöffnet.



8. Wählen Sie einen privaten Schlüssel aus den privaten Schlüsseln auf dem lokalen Schlüsselbund aus und geben Sie das entsprechende Passwort ein (wenn das Passwort nicht zwischengespeichert wurde). Dieser Schlüssel wird zur Sicherung der PGP NetShare Konfigurationsinformationen für den geschützten Ordner und die darin enthaltenen Dateien verwendet.

9. Klicken Sie auf **Weiter**. Die Fortschrittsanzeige erscheint.



Die Dateien im geschützten Ordner werden verschlüsselt und die angegebenen Benutzer sind zur Benutzung der Dateien berechtigt.

10. Klicken Sie auf **Fertig stellen**.

PGP WDE zur Verschlüsselung eines Laufwerks verwenden

Mit der Funktion PGP Whole Disk Encryption (WDE) kann der gesamte Inhalt Ihres Systems oder eines von Ihnen angegebenen externen oder USB-Flash-Laufwerks gesperrt werden.

Der von PGP WDE verwendete Verschlüsselungsalgorithmus ist AES256. Der Hashing-Algorithmus ist SHA-1. Mit FAT16, FAT32 und NTFS formatierte Laufwerke werden unterstützt. Es gibt keine minimale oder maximale Größe. Wenn das Laufwerk vom Betriebssystem (oder dem Hardware-BIOS für das Boot-Laufwerk) unterstützt wird, sollte es mit PGP WDE kompatibel sein.

Achtung: PGP Corporation empfiehlt als beste Praktik, dass Sie vor der Verschlüsselung des Laufwerks Ihre Daten sichern.

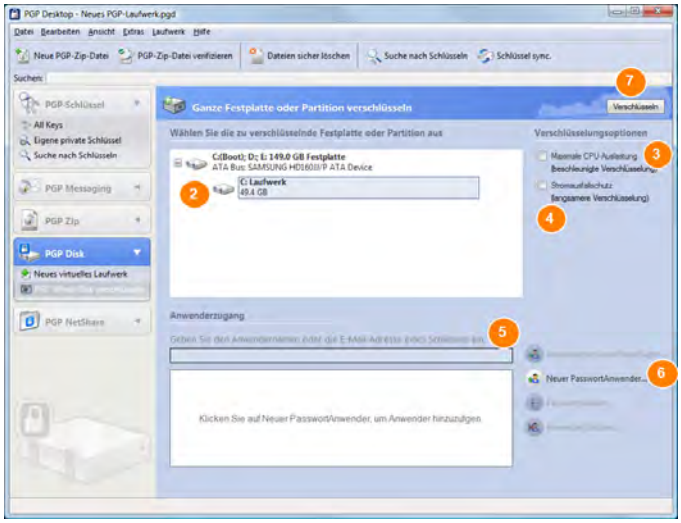
1. Klicken Sie auf **Gesamte Festplatte verschlüsseln** im Bedienfeld „PGP Disk“.

2. Wählen Sie das zu verschlüsselnde Laufwerk bzw. die Partition.
3. Wählen Sie **Maximale CPU-Nutzung**, um Ihr Laufwerk so schnell wie möglich zu schützen. Der Verschlüsselungsprozess hat Priorität vor den anderen Betriebsabläufen auf Ihrem System.
4. Wählen Sie **Stromausfallschutz**, wenn Sie befürchten, dass während des Verschlüsselungsprozesses ein Stromausfall auftreten könnte.

   Bei Auswahl von **Stromausfallschutz** kann der Verschlüsselungsprozess sicher wieder aufgenommen werden, wenn er unterbrochen wird. Diese Option kann zu einer längeren Ausführungszeit für die Verschlüsselung führen.
5. Klicken Sie auf **Anwenderschlüssel hinzufügen**, um Anwender hinzuzufügen, die die Fähigkeit haben werden, die Authentifizierung für das gesamte verschlüsselte Laufwerk über Kryptographie mit öffentlichem Schlüssel vorzunehmen.

   Bei Verschlüsselung einer Festplatte können Sie nur ein PGP-Schlüsselpaar auf einem Aladdin eToken USB-Token verwenden. Bei Verschlüsselung einer Partition oder eines Wechsellaufwerks (keine Festplatte) können Sie jedes Schlüsselpaar auf Ihrem System verwenden.
6. Klicken Sie auf **Neuer Passwortanwender**, um Anwender hinzuzufügen, die die Authentifizierung mit einem Passwort vornehmen und um ein USB-Laufwerk zur zweifaktoriellen Authentifizierung zu verwenden. Folgen Sie der Anleitung, die im Dialogfeld PGP Disk- Assistent angezeigt wird.

   Bei Verschlüsselung Ihres Boot-Laufwerks haben Sie die Option, Ihr Passwort zur Anmeldung für Windows zu verwenden, so dass Sie Ihre Anmeldedaten nur einmal beim Systemstart einzugeben brauchen.
7. Klicken Sie auf **Verschlüsseln**.



Hinweise: Zur Verschlüsselung von Daten auf Disketten oder CD-RWs verwenden Sie PGP Virtual Disk-Laufwerke, aber niemals PGP WDE.

Sie können PGP Whole Disk Encryption nur dann mit einem Dual-Boot-System verwenden, wenn Sie das System mit einem Betriebssystem starten, das durch PGP WDE unterstützt wird (zum Beispiel Windows XP, Windows 2000 oder Windows Vista), und PGP Whole Disk Encryption installiert ist. Der Partitionsmodus unterstützt Dual-Boot mit einem anderen Betriebssystem (zum Beispiel Linux) nur dann, wenn Sie nur die Windows-Partition verschlüsseln. Dieses andere

Betriebssystem muß sich allerdings auf einer anderen, nicht verschlüsselten Partition befinden.

Sicherungssoftware funktioniert in der Regel mit PGP WDE; alle von der Software gesicherten Dateien werden *vor* dem Anlegen der Sicherungskopie entschlüsselt.

Beste PGP WDE – Bewährte Methoden

PGP Corporation empfiehlt die folgenden bewährten Methoden zur Vorbereitung der Verschlüsselung Ihres Laufwerks mit PGP WDE. Bitte befolgen Sie die nachstehenden Empfehlungen zum Schutz Ihrer Daten während und nach der Verschlüsselung.

Vor der Verschlüsselung des Laufwerks müssen Sie einige Schritte ausführen, um die erfolgreiche Erstverschlüsselung des Laufwerks sicherzustellen.

1. **Vergewissern Sie sich, dass Ihr Ziellaufwerk unterstützt wird.** Die PGP WDE-Funktion schützt Desktop- oder Laptop-Laufwerke (entweder Partitionen oder das gesamte Laufwerk), externe Laufwerke und USB-Flash-Laufwerke. CD-RW/DVD-RWs und Server werden *nicht* unterstützt. Siehe „Unterstützte Laufwerktypen" im *Benutzerhandbuch für PGP Desktop* für weitere Einzelheiten zu den unterstützten Laufwerktypen.
2. **Sichern Sie das Laufwerk, bevor Sie es verschlüsseln.** Sichern Sie das Laufwerk vor der Verschlüsselung, damit keine Daten verloren gehen, wenn der Laptop oder Computer verloren geht, gestohlen wird oder Sie das Laufwerk nicht entschlüsseln können.
3. **Stellen Sie vor dem Verschlüsseln sicher, dass sich das Laufwerk in einwandfreiem Zustand befindet.** Falls PGP WDE während der Verschlüsselung Laufwerksfehler erkennt, hält das Programm an, damit die Probleme behoben werden können. Es ist jedoch effizienter, die Fehlerbehebung vor der Erstverschlüsselung vorzunehmen. Siehe *Einwandfreien Zustand des Laufwerks vor der Verschlüsselung sicherstellen* (Seite 9) für weitere Informationen.
4. **Erstellen Sie einen Wiederherstellungsdatenträger.** Obwohl die Wahrscheinlichkeit äußerst gering ist, dass ein Master-Boot-Datensatz auf einem mit PGP Whole Disk Encryption verschlüsselten Boot-Laufwerk bzw. einer Partition beschädigt wird, kann dies nicht ausgeschlossen werden. Erstellen Sie, bevor Sie ein Laufwerk oder eine Partition mit PGP Whole Disk Encryption verschlüsseln, einen Wiederherstellungsdatenträger. Siehe *Eine Wiederherstellungs-CD erstellen (Seite 10)* für eine Anleitung zur Erstellung eines Wiederherstellungsdatenträgers.
5. **Stellen Sie sicher, dass Ihnen für die Dauer der Verschlüsselung eine Netzstromversorgung zur Verfügung steht.** Siehe *Netzstromversorgung im Verlauf der Verschlüsselungaufrechterhalten* (Seite 10).
6. **Führen Sie einen Versuchstest aus, um die Softwarekompatibilität sicherzustellen.** PGP Corporation empfiehlt als gute Sicherheitspraxis, PGD WDE auf einer kleinen Gruppe von Computern zu testen, um sicherzustellen, dass kein Konflikt zwischen PGP WDE und anderer Software auf dem Computer besteht, bevor es auf einer großen Gruppe von Computern bereitgestellt wird. Das ist besonders nützlich in Umgebungen, die ein standardisiertes Corporate Operating Environment (COE)-Bild verwenden. Für eine Liste der Software mit bekannten Kompatibilitätsproblemen mit PGP WDE siehe *Einen Pilottests zur Sicherstellung der Softwarekompatibilität ausführen* (Seite 10).
7. **Durchführung einer Laufwerkwiederherstellung auf entschlüsselten Laufwerken.** Wenn Laufwerkwiederherstellungsaktivitäten an einem mit PGP Whole Disk Encryption (WDE) geschützten Wechseldatenträger vorgenommen werden müssen, empfiehlt PGP Corporation als beste Praktik die vorherige Entschlüsselung des Laufwerks. Nehmen Sie das mit Hilfe von **Laufwerk > Entschlüsseln** in PGP Desktop unter Einsatz Ihres vorbereiteten PGP WDE Wiederherstellungsdatenträgers oder durch Anschluss der Festplatte mit einem USB-Kabel an einem zweiten System und Entschlüsselung über die PGP Desktop-Software dieses Systems vor. Setzen Sie die Wiederherstellung nach der Entschlüsselung fort.

Die Laufwerksintegrität vor der Verschlüsselung sicherstellen

PGP Corporation nimmt bewusst eine konservative Haltung bei der Laufwerkverschlüsselung ein, um Datenverlust zu verhindern. Bei der Verschlüsselung von Festplatten treten nicht selten CRC (Cyclic Redundancy Check)-Fehler auf. Wenn PGP WDE eine Festplatte oder Partition mit beschädigten Sektoren feststellt, wird der Verschlüsselungsprozess standardgemäß unterbrochen. Während dieser Pause können Sie das Problem beheben, bevor Sie den Verschlüsselungsprozess fortsetzen, und auf diese Weise mögliche Laufwerkbeschädigung und Datenverlust verhindern.

Um eine Unterbrechung der Verschlüsselung zu verhindern, empfiehlt PGP Corporation, vor der Verschlüsselung alle Laufwerkfehler zu korrigieren, um mit einem Laufwerk mit einwandfreier Integrität zu beginnen.

- Es empfiehlt sich vor dem Versuch, PGP WDE zu verwenden, ein Festplatten-Dienstprogramm eines Drittherstellers zu verwenden. Dieses Dienstprogramm muss die Fähigkeit haben, eine Low-Level-Integritätskontrolle durchzuführen und alle Unregelmäßigkeiten des Laufwerks, die zu CRC-Fehlern führen könnten, zu reparieren. Das Checkdisk-Programm von Disk Microsoft Windows (chkdsk.exe) reicht nicht aus, um diese Probleme auf dem Ziellaufwerk festzustellen. Verwenden Sie stattdessen Software wie SpinRite oder Norton Disk Doctor™. Diese Softwareanwendungen können Fehler korrigieren, die ansonsten die

Verschlüsselung unterbrechen würden.

- Es hat sich bewährt, stark fragmentierte Laufwerke vor der Verschlüsselung zu defragmentieren.

Eine Wiederherstellungs-CD erstellen:

Die folgende Anleitung verwendet Roxio-Software für Illustrationszwecke. Die tatsächlich von Ihnen durchgeführten Schritte können abweichend sein.

1. Vergewissern Sie sich, dass PGP Desktop und Roxio Easy Media Creator oder Roxio Easy CD Creator (oder eine andere Software, die eine CD aus einem ISO-Image erstellen kann) auf Ihrem System installiert sind.
2. Öffnen Sie Roxio Easy Media Creator bzw. Roxio Easy CD Creator und wählen Sie die Option zur Erstellung eines Daten-CD-Projekts aus.
3. Wählen Sie **File (Datei) > Record CD from CD Image (CD über CD-Imgae aufnehmen)**.
4. Wählen Sie im Menü **Files of Type (Dateityp)** die Option **ISO Imgae Files (ISO-Image-Dateien) aus**.
5. Navigieren Sie zum PGP-Verzeichnis. Der Standardspeicherort ist `C:\Programme\PGP Corporation\PGP Desktop\`.
6. Wählen Sie `bootg.iso` aus und klicken Sie auf **Öffnen**.
7. Legen Sie eine leere, beschreibbare CD in das CD-Laufwerk ein.
8. Klicken Sie im Bildschirm Record CD Setup (CD-Aufzeichnung-Setup) auf **Start Recording (Aufzeichnung starten)**.
9. Wenn die Datei auf der CD registriert ist, klicken Sie auf **OK**.
10. Nehmen Sie die Wiederherstellungs-CD aus dem Laufwerk und beschriften Sie sie entsprechend.

Achtung: PGP WDE-Wiederherstellungsdatenträger sind nur mit der Version von PGP Desktop kompatibel, mit der die Wiederherstellungs-CD erstellt wurde. Wenn Sie z. B. versuchen, mit einer in Version 9.0.x erstellten Wiederherstellungs-CD ein durch PGP WDE 9.7 geschütztes Laufwerk zu entschlüsseln, kann nicht mehr auf das PGP WDE 9.7-Laufwerk zugegriffen werden.

Netzbetrieb während der Verschlüsselung beibehalten

Weil die Verschlüsselung ein CPU-intensiver Prozess ist, kann keine Verschlüsselung auf einem Laptop, der im Akkubetrieb angeschlossen ist, gestartet werden. Der Computer *muss* über das Netzteil mit Strom versorgt werden. Wenn Sie einen Laptop während der erstmaligen Verschlüsselung (oder der späteren Entschlüsselung bzw. Umschlüsselung) in den Akkubetrieb umschalten, wird die PGP WDE-Aktivität angehalten. Die Verschlüsselung, Entschlüsselung oder Umschlüsselung wird automatisch fortgesetzt, sobald der Computer wieder über das Netzteil mit Strom versorgt wird.

Unabhängig vom verwendeten Computertyp darf während der Verschlüsselung die Stromversorgung nicht unterbrochen oder das System anderweitig unerwartet herunterfahren werden, sofern Sie nicht die Option „Stromausfallschutz“ ausgewählt haben.

Ziehen Sie das Netzkabel auf keinen Fall ab, bevor der Verschlüsselungsvorgang abgeschlossen ist. Wenn es während der Verschlüsselung zu einem Stromausfall kommen kann—oder wenn keine unterbrechungsfreie Stromversorgung für Ihren Computer existiert—sollten Sie die Option „Stromausfallschutz“ aktivieren, die im *Benutzerhandbuch für PGP Desktop* beschrieben ist.

Achtung: Dies gilt ebenfalls für Wechseldatenträger, wie zum Beispiel USB-Geräte. Wenn die Option „Stromausfallschutz“ nicht ausgewählt ist, laufen Sie Gefahr, dass das Gerät beschädigt wird, wenn Sie es während der Verschlüsselung entfernen.

Versuchstest zur Sicherstellung der Softwarekompatibilität ausführen

Es gibt andere Arten von Laufwerkschutz-Software, die nicht mit PGP WDE kompatibel sind und schwerwiegende Laufwerkprobleme verursachen können, einschließlich Datenverlust.

Bitte beachten Sie die folgenden bekannten Interoperabilitätsprobleme und lesen Sie die neusten Updates dieser Liste in den PGP Desktop-Versionshinweisen.

Inkompatible Software:

- Faronics Deep Freeze (alle Ausgaben)
- Utimaco Safeguard Easy 3.x
- Produkte zur Festplattenverschlüsselung von GuardianEdge Technologies: Dies betrifft die früher unter der Bezeichnung „PC Guardian“ vertriebenen Produkte „Encryption Anywhere Hard Disk“ und „Encryption Plus Hard Disk“.

Die folgenden Anwendungen können mit PGP Desktop auf demselben System installiert werden, blockieren jedoch die Funktion von PGP Whole Disk Encryption:

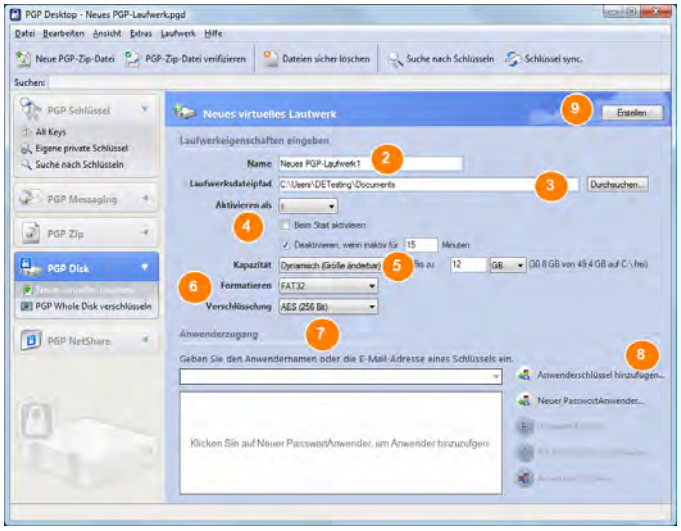
- Safeboot Solo
- SecureStar SCPP

PGP Virtual Disk-Laufwerke erstellen

Die Funktion PGP Virtual Disk-Datenträger verwendet einen Teil Ihres Festplattenspeichers als verschlüsseltes virtuelles Laufwerk mit seinem eigenen Laufwerksbuchstaben. Sie können weitere Anwender für ein Laufwerk erstellen und dadurch autorisierten Personen den Zugriff gestatten.

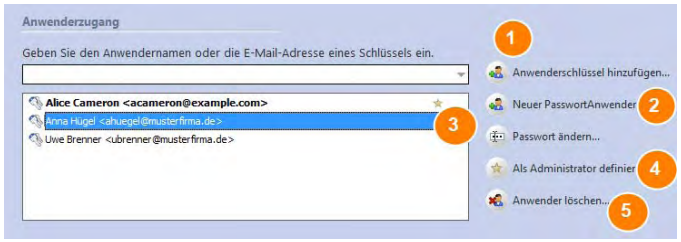
1. Klicken Sie auf **Neues Virtual Disk-Laufwerk** im Bedienfeld „PGP Disk“.

2. Geben Sie einen **Namen** für das Laufwerk ein.
3. Geben Sie einen **Laufwerksdateipfad** für das Laufwerk ein.
4. Geben Sie Ihre Aktivierungspräferenzen wie folgt an:
   - wählen Sie unter **Aktivieren als** einen Laufwerksbuchstaben für das Laufwerk aus..
   - wählen Sie **Beim Start aktivieren**, damit Ihr neues Laufwerk automatisch beim Start aktiviert wird.
   - wählen Sie **Deaktivieren wenn inaktiv für x Minuten** , wenn das Laufwerk automatisch deaktiviert werden soll, wenn es für die Dauer der angegebenen Minuten inaktiv war.
5. Wählen Sie unter **Kapazität** die Option **Dynamisch (Größe änderbar)**, wenn Sie wollen, dass die Größe des Laufwerks zunimmt, wenn Sie Dateien hinzufügen, oder wählen Sie **Feste Größe**, wenn Sie wollen, dass das Laufwerk immer die gleiche Größe hat.
6. Geben Sie unter **Format** ein Dateisystemformat für das Laufwerk an.
7. Geben Sie unter **Verschlüsselung** den Verschlüsselungsalgorithmus für das Laufwerk an.
8. Klicken Sie auf **Anwenderschlüssel hinzufügen**, um Benutzer hinzuzufügen, die die Authentifizierung über Kryptographie mit öffentlichem Schlüssel vornehmen, oder klicken Sie auf **Neuer Passwortanwender**, um Anwender hinzuzufügen, die die Authentifizierung mit Passwörtern vornehmen.
9. Klicken Sie auf **Erstellen**.



Verwenden Sie den Abschnitt **Anwenderzugang** zur Kontrolle von bestehenden Benutzern eines PGP Virtual Disk-Laufwerks:

1. Klicken Sie auf **Anwenderschlüssel hinzufügen**, um Benutzer hinzuzufügen, die die Authentifizierung über Kryptographie mit öffentlichem Schlüssel vornehmen.
2. Klicken Sie auf **Neuer Passwortanwender**, um Anwendzer hinzuzufügen, die die Authentifizierung mit Passwörtern vornehmen.
3. Wählen Sie einen Passwortanwender und klicken Sie dann auf **Passwort ändern**, um sein Passwort zu ändern.
4. Wählen Sie einen Anwender und klicken Sie dann auf **Als Administrator definieren**, um dem Anwender Administratorrechte zu verleihen.
5. Wählen Sie einen Anwender und klicken Sie dann auf **Löschen**, um ihn zu löschen.



PGP Zip-Archive erstellen

Mit PGP Zip-Archiven können Sie beliebige Kombinationen von Dateien und Ordnern in ein komprimiertes, portables Archiv setzen. Es gibt vier Arten von PGP Zip-Archiven:

- **Empfängerschlüssel**. Verschlüsselt das Archiv für öffentliche Schlüssel. Nur der Inhaber der entsprechenden privaten Schlüssel kann das Archiv öffnen. Dies ist der

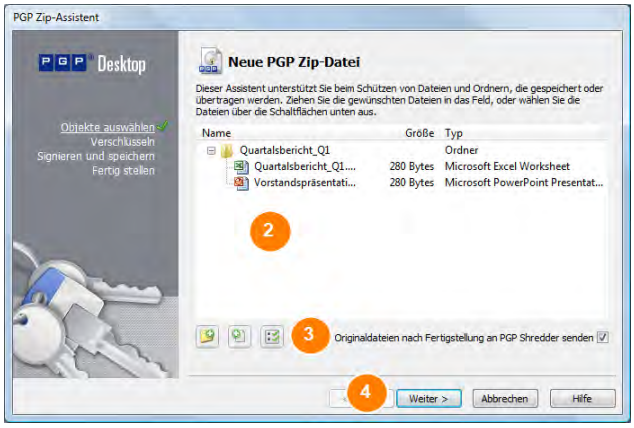
sicherste Typ eines PGP Zip-Archivs. Die Empfänger müssen PGP Desktop (für Windows oder Mac OS X) verwenden.

- **Passwort**. Verschlüsselt das Archiv für ein Passwort, das den Empfängern mitgeteilt werden muss. Die Empfänger müssen PGP-Software (für Windows oder Mac OS X) verwenden.
- **Selbstentschlüsselndes PGP-Archiv**. Verschlüsselt das Archiv für ein Passwort. Empfänger benötigen zum Öffnen keine PGP-Software, sie müssen jedoch Windows oder Mac OS X auf ihrem Computer ausführen. Das Passwort muss den Empfängern mitgeteilt werden.
- **Nur signieren**. Signiert das Archiv, ohne es zu verschlüsseln, und ermöglicht Ihnen so den Nachweis, dass Sie der Absender sind. Die Empfänger müssen PGP-Software verwenden (für Windows oder Mac OS X), um das Archiv öffnen und verifizieren zu können.

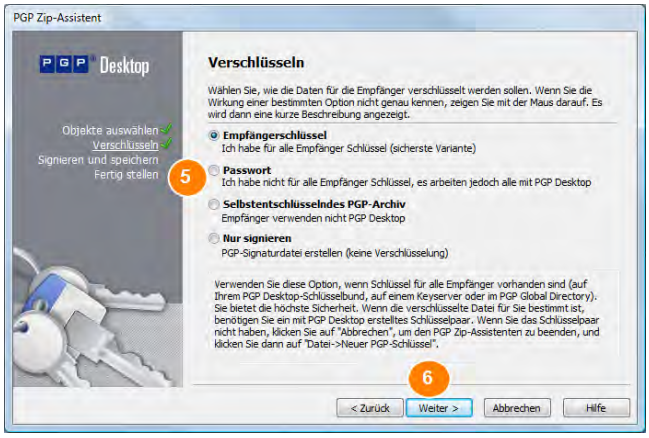
Die PGP Zip-Typen „Passwort" und „Nur signieren" sind im *PGP Desktop Anwenderhandbuch* näher beschrieben; sie werden daher hier nur kurz angesprochen.

1. Klicken Sie auf **Neues PGP Zip** im Bedienfeld „PGP Zip".

2. Ziehen und legen Sie die gewünschten Dateien/Ordner im Archiv ab oder wählen Sie sie mit Hilfe der Schaltflächen aus.
3. Wählen Sie **Originaldateien nach Fertigstellung an PGP Shredder senden**, wenn Sie wollen, dass die von Ihnen in das Archiv gesetzten Dateien/Ordner nach Erstellung des Archivs sicher gelöscht werden.
4. Klicken Sie auf **Weiter**.



5. Wählen Sie den gewünschten Typ des PGP Zip-Archivs:
   - **Empfängerschlüssel**
   - **Passwort**
   - **Selbstentschlüsselndes PGP-Archiv**
   - **Nur signieren**
6. Klicken Sie auf **Weiter**.



Die Typen **Passwort** und **Nur signieren** sind im *PGP Desktop Anwenderhandbuch* näher beschrieben.

Beziehen Sie sich auf den entsprechenden Abschnitt auf den folgenden Seiten für Informationen zum von Ihnen angegebenen PGP Zip-Archivtyp.

Empfängerschlüssel

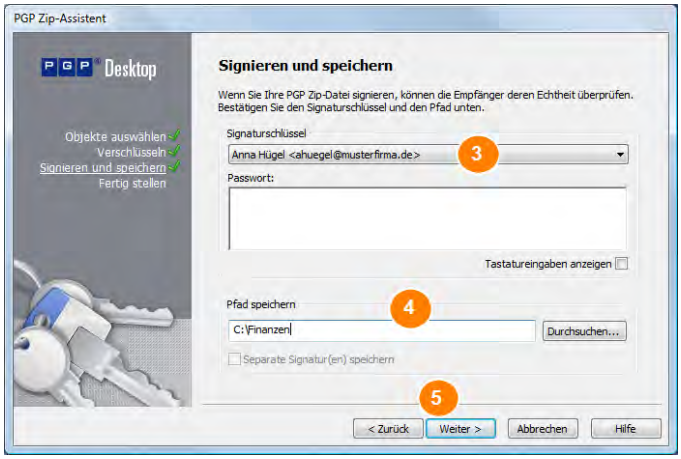
Der Bildschirm „Anwenderschlüssel hinzufügen" erscheint.

1. Klicken Sie auf **Hinzufügen** und verwenden Sie den Bildschirm „Anwenderauswahl", um die öffentlichen Schlüssel der Personen auszuwählen, die Sie zur Öffnung des Archivs befähigen wollen. Damit Sie das Archiv auch selbst öffnen können, müssen Sie auch Ihren öffentlichen Schlüssel mit aufnehmen.
2. Klicken Sie auf **Weiter**.

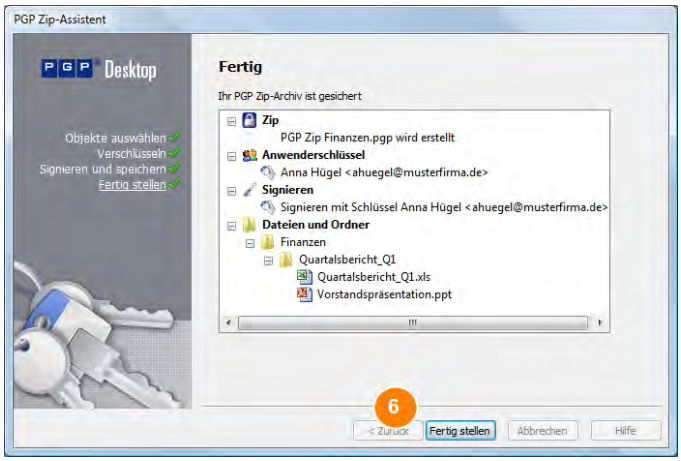
3. Wählen Sie einen privaten Schlüssel auf dem lokalen System, den Sie zur Signatur des Archivs verwenden.
4. Geben Sie einen Namen und einen Speicherort für das Archiv an. Der Standardname ist der Name der ersten Datei bzw. Ordners im Archiv; der Standardspeicherort ist der Speicherort der Dateien/Ordner, die in das

Archiv gesetzt werden.

5. Klicken Sie auf **Weiter**. Das PGP Zip-Archiv wird erstellt. Der Bildschirm „Beendet“ zeigt Informationen über das neue Archiv an.



6. Klicken Sie auf **Fertig stellen**.



Hinweis: Der Passwort-Typ des PGP Zip-Archivs ist dem Typ Empfängerschlüssel sehr ähnlich; der einzige Unterschied ist, dass ein Passwort statt eines Schlüssels zum Schutz des Archivs verwendet wird.

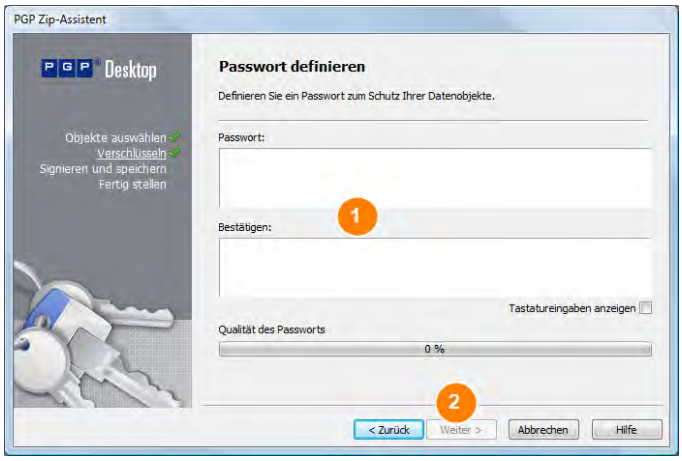
Hinweis: Der Typ „Nur signieren“ des PGP Zip-Archivs ist dem Typ Empfängerschlüssel sehr ähnlich; der einzige Unterschied ist, dass Sie keine öffentlichen Schlüssel auswählen, weil das Archiv lediglich signiert, jedoch nicht verschlüsselt wird.

Selbstentschlüsselndes PGP-Archiv

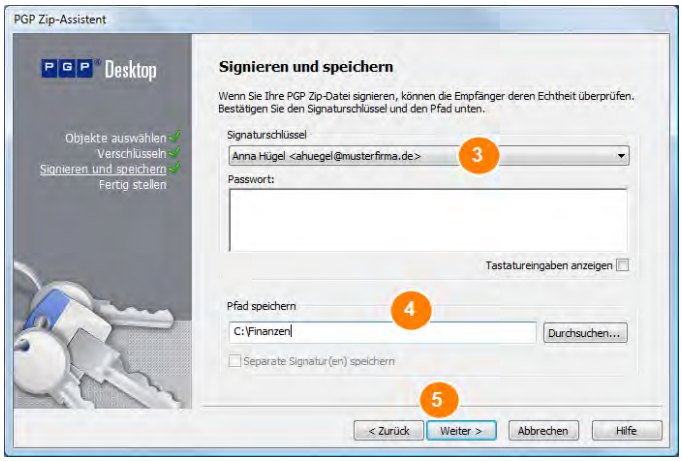
Der Bildschirm „Passwort definieren“ wird geöffnet.

1. Geben Sie ein Passwort für das PGP Zip Selbstentschlüsselnde Archiv (SDA) ein und bestätigen Sie es, indem Sie es erneut eingeben.

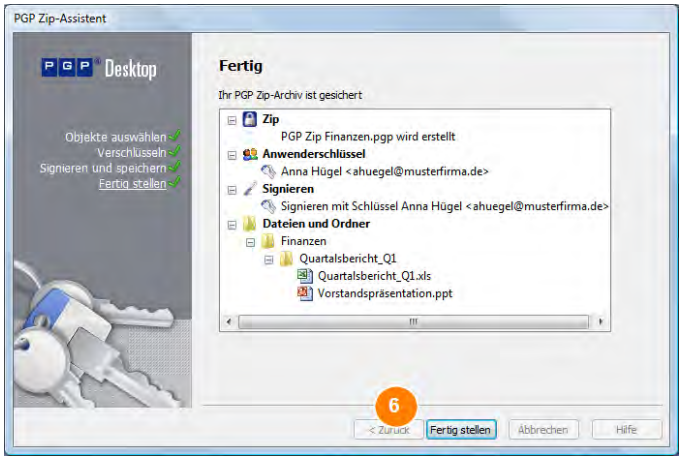
2. Klicken Sie auf **Weiter**.



3. Wählen Sie einen privaten Schlüssel auf dem lokalen System, den Sie zur Signatur des Archivs verwenden.
4. Geben Sie einen Namen und einen Speicherort für das Archiv an. Der Standardname ist der Name der ersten Datei bzw. Ordners im Archiv; der Standardspeicherort ist der Speicherort der Dateien/Ordner, die in das Archiv gesetzt werden.
5. Klicken Sie auf **Weiter**. Das PGP SDA wird erstellt.



6. Klicken Sie auf **Fertig stellen**.



PGP Shred zur sicheren Löschung von Dateien verwenden

Die Funktion PGP Shredder vernichtet Dateien und Ordner vollständig, so dass sie selbst mit hochentwickelter Datei-wiederherstellungssoftware nicht wiederhergestellt werden können. Obwohl das PGP Shredder-Symbol wie auch der Windows-Papierkorb auf Ihrem Desktop erscheinen, werden die angegebenen Dateien nur von PGP Shredder sofort überschrieben, so dass sie nicht wiederherstellbar sind.

Die sichere Löschung von Dateien ist mit jedem der folgenden Verfahren möglich:

- Über das PGP Shredder-Symbol
- Über die PGP-Symbolleiste
- Über das PGP-Kontextmenü

Dateien mit dem PGP Shredder-Symbol sicher löschen

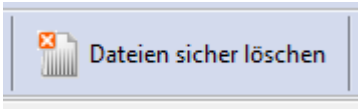
➢ So löschen Sie Dateien mit dem PGP Shredder-Symbol sicher

1. Ziehen Sie auf dem Windows-Desktop die Dateien und Ordner, die Sie sicher löschen wollen, in den PGP Shredder. Im nun erscheinenden Dialogfeld werden Sie aufgefordert zu bestätigen, dass Sie die Dateien sicher löschen wollen.
2. Klicken Sie auf **Ja**. Die angegebenen Dateien und Ordner werden nun sicher gelöscht.

Dateien mit der PGP-Symbolleiste sicher löschen

➢ So löschen Sie Dateien mit der PGP-Symbolleiste sicher

1. Öffnen Sie PGP Desktop.
2. Klicken Sie auf **Dateien sicher löschen** auf der PGP-Symbolleiste.
3. Geben Sie die Dateien an, die Sie sicher löschen wollen. Klicken Sie bei gedrückter STRG-Taste, um mehrere Dateien auszuwählen, oder markieren Sie mit STRG-A alle angezeigten Dateien.
4. Klicken Sie auf **Öffnen**. Im nun erscheinenden Dialogfeld werden Sie aufgefordert zu bestätigen, dass Sie die Dateien sicher löschen wollen.
5. Klicken Sie auf **Ja**. Die angegebenen Dateien und Ordner werden nun sicher gelöscht.



Dateien mit dem PGP-Kontextmenü sicher löschen

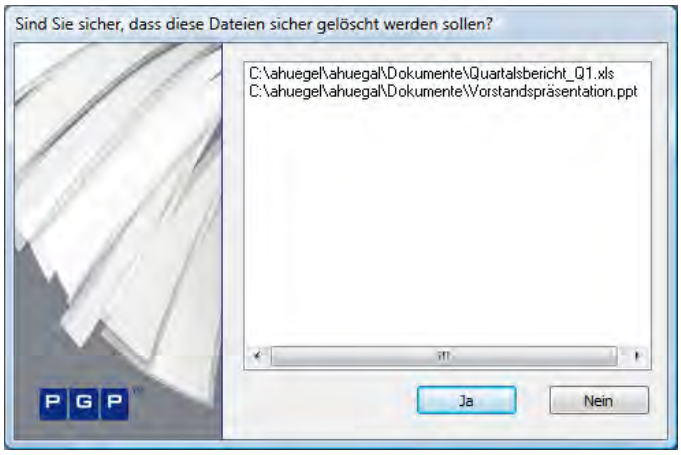
➢ So löschen Sie Dateien sicher in Windows Explorer

1. Öffnen Sie Windows Explorer.
2. Rechtsklicken Sie auf die Dateien oder Ordner, die Sie sicher löschen wollen, und wählen Sie dann **PGP Desktop > PGP Shred <Dateiname>**. Klicken Sie bei gedrückter STRG-Taste, um mehrere Dateien auszuwählen, oder markieren Sie mit STRG-A alle angezeigten Dateien.

Tipp: Wenn Sie mehr als eine Datei ausgewählt haben, erscheint der Text **PGP Shred x Objekte**, wobei **x** die Anzahl der ausgewählten Dateien ist.

Im nun erscheinenden Dialogfeld werden Sie aufgefordert zu bestätigen, dass Sie die Dateien sicher löschen wollen.

3. Klicken Sie auf **Ja**. Die angegebenen Dateien und Ordner werden nun sicher gelöscht.



Hinweis: Wenn Sie die Funktion PGP Shredder nicht oft benutzen, können Sie das PGP Shredder-Symbol vom Desktop mit PGP Optionen entfernen. Wählen Sie dazu **Extras > ptionen**, wählen Sie dann die Registerkarte „Laufwerk“, deselektieren Sie die Option **PGP Shredder-Symbol auf dem Desktop platzieren** und klicken Sie dann auf **OK**.

Hinweis: Sie können auch die PGP-Optionen verwenden, um die Anzahl der bei der sicheren Löschung vorgenommenen Durchgänge zu steuern (mehrere Durchgänge sind sicherer, dauern jedoch länger). Sie können hier auch angeben, ob die Dateien im Windows-Papierkorb bei der Leerung sicher gelöscht werden sollen und ob das Warndialogfeld erscheinen soll, wenn Sie die sichere Löschung vornehmen.

Freien Speicherplatz sicher löschen

Die Funktion PGP Shred Free Space (Freien Speicherplatz sicher löschen) löscht freien Speicherplatz auf Ihren Laufwerken, so dass Ihre gelöschten Daten definitiv nicht wiederherstellbar sind. Es ist zu beachten, dass „freier Speicherplatz“ eigentlich eine falsche Bezeichnung ist. PGP Shred Free Space überschreibt die Teile Ihrer Festplatte, die Windows für leer hält; der Speicherplatz kann jedoch leer sein oder Dateien umfassen, die nach Angabe von Windows gelöscht wurden.

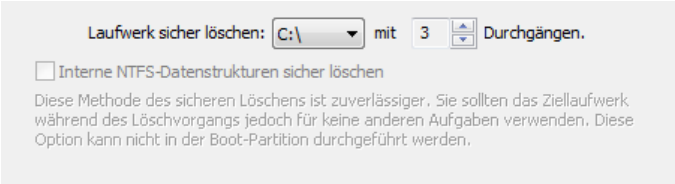
Wenn Sie Dateien in den Windows-Papierkorb ablegen und ihn leeren, werden die Dateien nicht wirklich gelöscht; Windows tut nur so, als ob sich dort nichts befindet und überschreibt die Dateien schließlich. Aber bis diese Dateien überschrieben werden, können sie leicht von einem Angreifer wiederhergestellt werden. PGP Shred Free Space überschreibt jedoch diesen „freien Speicherplatz“, so dass diese Dateien selbst mit Wiederherstellungssoftware nicht wiederhergestellt werden können.

➢ So löschen Sie sicher freien Speicherplatz auf Ihren Laufwerken

1. Öffnen Sie PGP Desktop.
2. Wählen Sie **Extras > Freien Speicherplatz sicher löschen**.
3. Lesen Sie die einführenden Informationen und klicken Sie dann auf **Weiter**
4. Wählen Sie im Feld **Laufwerk sicher löschen**, auf dem Bildschirm „Informationen sammeln“, das Laufwerk oder den Datenträger, das bzw. den Sie sicher löschen wollen, sowie die Anzahl der Durchgänge, die PGP Shred für freien Speicherplatz ausführen soll.

   Die empfohlenen Richtlinien für Durchgänge sind:

   - 3 Durchgänge für den persönlichen Gebrauch
   - 10 Durchgänge für den geschäftlichen Gebrauch
   - 18 Durchgänge für den militärischen Gebrauch
   - 26 Durchgänge für maximale Sicherheit

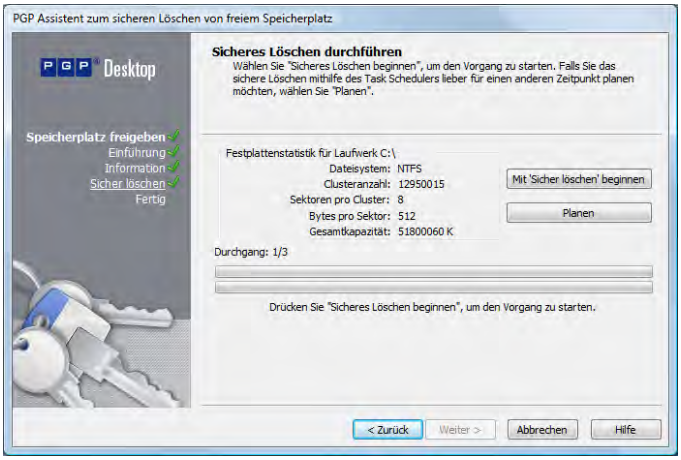

Laufwerk sicher löschen: C:\ mit 3 Durchgängen.
Interne NTFS-Datenstrukturen sicher löschen
Diese Methode des sicheren Löschens ist zuverlässiger. Sie sollten das Zielaufwerk während des Löschvorgangs jedoch für keine anderen Aufgaben verwenden. Diese Option kann nicht in der Boot-Partition durchgeführt werden.

5. Wählen Sie ggf. die Option **Interne NTFS-Datenstrukturen sicher löschen** (nicht auf allen Systemen verfügbar) und klicken Sie dann auf **Weiter**.

   Diese Option löscht sicher kleine Dateien (unter 1KB) in internen Datenstrukturen, die anderenfalls nicht sicher gelöscht werden würden.
6. Klicken Sie auf dem Bildschirm „Sicheres Löschen durchführenn“ auf **Sicheres Löschen beginnen**.

Hinweis: Klicken Sie auf **Planen**, wenn Sie einen Zeitpunkt für die sichere Löschung Ihres freien Speicherplatzes ansetzen wollen, anstatt diese jetzt durchzuführen. Der Windows-Taskplaner muss dazu auf Ihrem System installiert sein.

Die Dauer des sicheren Löschens hängt von der Anzahl der angegebenen Durchgänge, der Geschwindigkeit der CPU, der Anzahl der ausgeführten anderen Anwendungen usw. ab.


PGP Assistent zum sicheren Löschen von freiem Speicherplatz
PGP Desktop
Speicherplatz freigeben
Einführung
Information
Sicher löschen
Fertig
Sicheres Löschen durchführen
Wählen Sie "Sicheres Löschen beginnen", um den Vorgang zu starten. Falls Sie das sichere Löschen mithilfe des Task Schedulers lieber für einen anderen Zeitpunkt planen möchten, wählen Sie "Planen".
Festplattenstatistik für Laufwerk C:\
Dateisystem: NTFS
Clusteranzahl: 12950015
Sektoren pro Cluster: 8
Bytes pro Sektor: 512
Gesamtkapazität: 51800060 K
Mit 'Sicher löschen' beginnen
Planen
Durchgang: 1/3
Drücken Sie "Sicheres Löschen beginnen", um den Vorgang zu starten.
< Zurück
Weiter >
Abbrechen
Hilfe

7. Klicken Sie nach Abschluss des sicheren Löschens auf **Weiter**.
8. Klicken Sie auf dem Bbildschirm „Abschliessen“ auf **Beenden**.

Hilfe und Support

Kontaktaufnahme mit dem technischen Support

- Wenn Sie sich über die PGP-Supportoptionen informieren oder Kontakt mit dem technischen Support der PGP Corporation aufnehmen möchten, besuchen Sie bitte die *PGP Corporation Support Home Page* http://www.pgp.com/support
- Auf der Website des *PGP Support-Portals* (https://support.pgp.com) können Sie auf die PGP Support-Wissensdatenbank zugreifen und PGP Technical Support anfordern. **Beachten Sie, dass Sie bestimmte Teile der PGP Support Knowledge Base ohne Support-Vertrag nutzen können; der technische Support kann Ihre Anfrage jedoch nur bearbeiten, wenn ein gültiger Supportvertrag besteht.**
- Alle weiteren Kontaktinformationen für die PGP Corporation finden Sie auf der *PGP Kontakt-Seite* (http://www.pgp.com/company/contact/index.html).
- Allgemeine Informationen über die PGP Corporation finden Sie auf der PGP-Website (http://www.pgp.com).
- Über die PGP Support-Website können Sie auf die *PGP Support-Foren zugreifen* (http://forums.pgpsupport.com). Hierbei handelt es sich um Support-Foren der Anwen-

dergemeinde, die von der PGP Corporation gehostet werden.

Verfügbare Dokumentation

Vor der Installation können Sie auf die vollständige Produktdokumentation über die *PGP Support-Wissensdatenbank* zugreifen (https://support.pgp.com/?faq=589).

Die PGP Desktop Dokumentation wird während der Installation auf Ihrem Rechner installiert. Um sie anzuzeigen, wählen Sie **Start > Programme > PGP > Dokumentation**. Alle Dokumente werden im PDF-Format (Adobe Acrobat Portable Document Format) gespeichert. Diese Dateien können mit Adobe Acrobat Reader, der auf der *Adobe-Website* (http://www.adobe.com) abrufbar ist, angezeigt und ausgedruckt werden. PGP Desktop enthält auch eine integrierte Windows Online-Hilfe.

Copyright

Copyright © 1991-2008 PGP Corporation. Alle Rechte vorfbehalten. „PGP“, „Pretty Good Privacy“ und das PGP-Logo sind in den Vereinigten Staaten von Amerika und anderen Ländern registrierte Warenzeichen der PGP Corporation. Alle eingetragenen und nicht eingetragenen Warenzeichen in diesem Dokument sind Eigentum Ihrer jeweiligen Eigentümer.